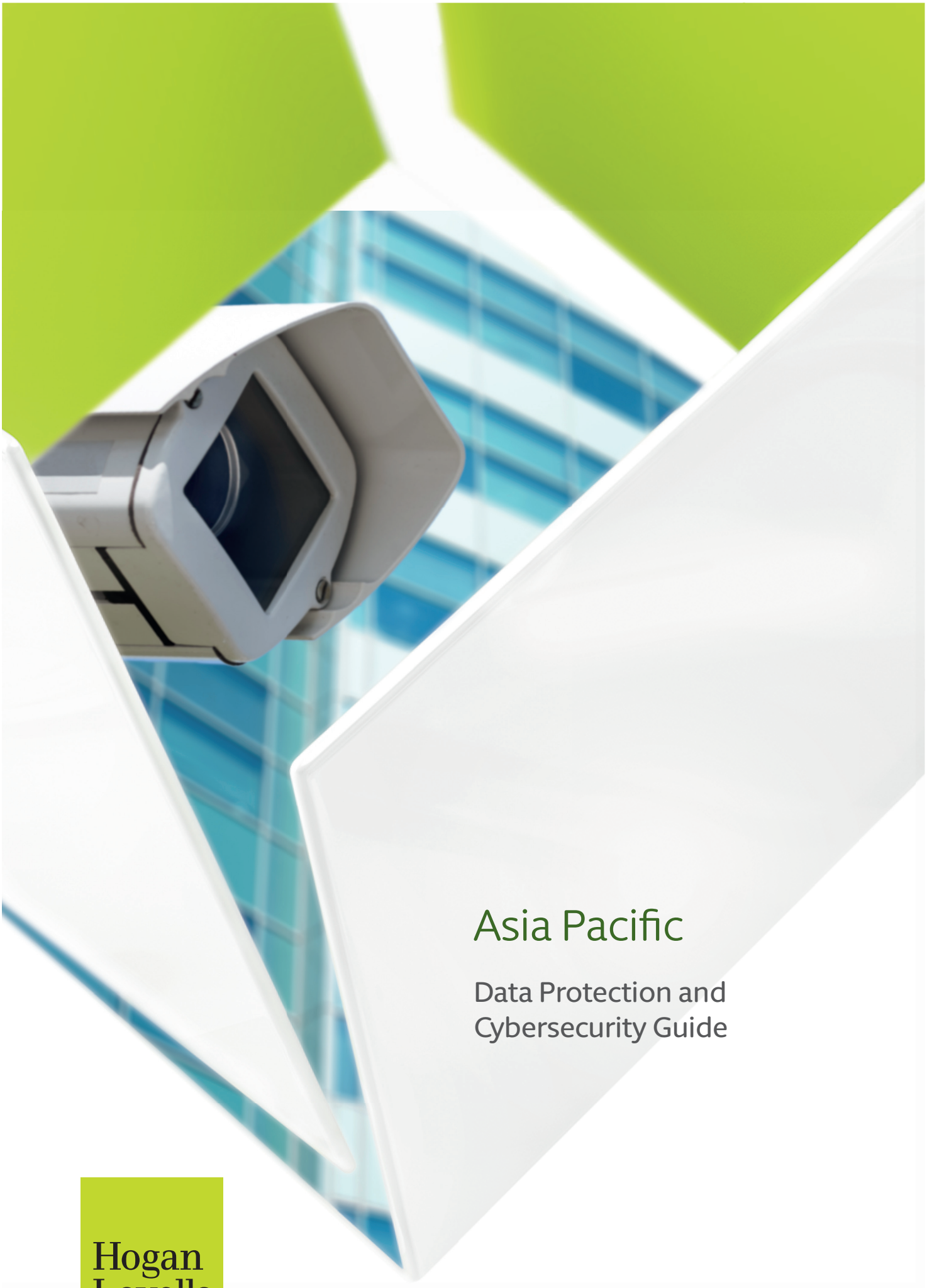
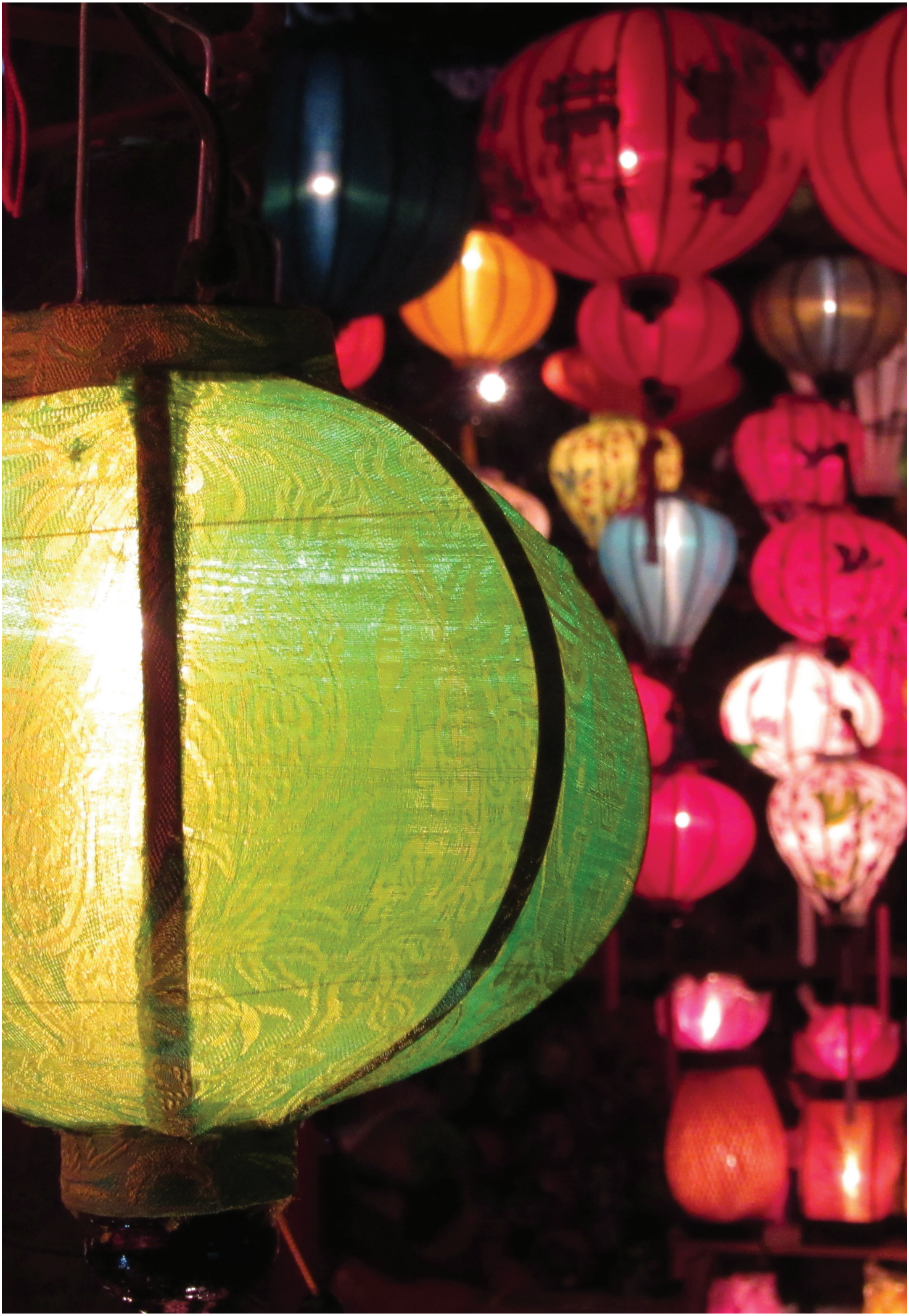


Asia Pacific

Data Protection and Cybersecurity Guide

Hogan Lovells



Contents

2016 – Data Protection and Cyber Security Regulation:

Shifting landscapes across the Asia-Pacific region

The initial push for comprehensive data protection regulation across the Asia-Pacific region that took hold between 2010 and 2015 has now run its course. During this period, the number of jurisdictions in the region with comprehensive "European-style" data protection regulatory regimes more than doubled from five to eleven, with new regimes coming into force in India, Malaysia, the Philippines, Singapore, South Korea and Taiwan.

Looking back on 2015 and forward to 2016, we see a new phase of regulatory development taking shape in the Asia-Pacific region. Some of the longer established laws are now being stepped up and we see a progression towards stricter, more punitive enforcement in a number of jurisdictions. As regulators settle into their new roles under recently enacted regimes, they are turning to publish more comprehensive and detailed compliance guidance and staffing up to administer enforcement. Critically, we see an important parallel development in cyber security regulation emerging across the region. The policy considerations relating to cyber security regulation often include data protection concerns, but often bring wider geopolitical and national security concerns into play.

Stepped up laws, more exacting compliance standards

2015 saw more onerous regulatory requirements under evaluation or introduced to a number of the more mature data protection regimes in the region:

- amendments to Japan's Personal Information Protection Act introduced a concept of "sensitive personal data", added data export controls and, critically, made provision for the appointment of a dedicated regulator;
- South Korea added punitive damages to its already stringent privacy laws;
- Taiwan introduced a concept of "sensitive personal data" to its Personal Data Protection Act; and
- Australia launched consultations towards introducing a mandatory data breach notification obligation to its Privacy Act.

There was also a general trend towards more demanding compliance environments across the region.

Hong Kong saw three convictions under its direct marketing offences. While the fines in these cases were relatively small (HK$10,000 in two cases and HK$30,000 in the third), all three prosecutions were widely publicized in the Hong Kong press, underscoring the growing reputational risks for failing to comply with Hong Kong's Personal Data (Privacy) Ordinance. Hong Kong's official enforcement statistics for 2015 showed a 16% increase in the number of complaints and a record high of 98 data breach notifications, up from 70 in 2014.

The Hong Kong and Singapore privacy regulators continued to be relatively prolific in their publication of detailed compliance guidance across a range of topics.

Looking forward to 2016, we expect to see the push towards comprehensive "European-style" data protection regulation to continue:

- Thailand's cabinet approved a new data protection and a cyber security law in January 2015, and these are proceeding through the legislative process; and
- Indonesia expects to introduce a new data protection law in early 2016.

At the time of printing, Malaysia had issued its Personal Data Protection Standards dealing with data security, integrity and retention requirements. Detailed direct marketing guidelines are expected later this year.

Singapore has announced that it will be publishing a Cyber Security Bill in the course of 2016.

Is Asia-Pacific harmonisation on the way?

At the moment, we do not yet see any clear trend towards common compliance standards across the region. Moving from a plain reading of the text of the newly enacted data protection laws (which in many respects appear similar across the region) to the practicalities of enforcement and compliance, we actually see increasing divergence as jurisdictions prescribe more and more detailed requirements, often with local nuance.

The APEC Privacy Framework has provided some rough signposts for a common approach to principles-based regulation, but priorities for policy-making and enforcement vary significantly by jurisdiction. These differences reflect different levels of economic development and political agendas, as well as different cultures and experiences with data protection issues.

While 2015 saw a general tightening of regulatory requirements across the region, there are some outliers. Malaysia and the Philippines still lack regulators responsible for administering their data protection laws, and this can reasonably be expected to be limiting in terms of the effective enforcement of the law. While Taiwan saw reforms to its laws directed at enhancing data protection standards, the removal of a number of offences from the law could be taken as a signal that aggressive enforcement will not be a priority.

With these differences emerging there is as yet no clear pathway towards conformity, through APEC or otherwise. It is clear that there is an increasingly pressing need to resolve differences in areas such as cross-border data transfer controls, which impact both businesses seeking to leverage regional and global operating platforms and regulators requesting or demanding data from other jurisdictions in support of compliance with anti-money laundering regulations and cross-border assistance with criminal investigations. A number of the national laws in the region, for example, provide for “white lists” of data transfer destination jurisdictions which are deemed to provide adequate standards of protection without any additional compliance measures being taken. However, in no case has a national authority issued a completed white list that would give effect to this intended flexibility.

Cyber Security – the emerging challenge

Asia-Pacific headlines reported on significant cyber security incidents throughout 2015, concluding the year with reports that Hong Kong-based toymaker Vtech had experienced a hacking in which the details of 5 million adults and over 6 million children had been compromised.

In addition to broader concerns about criminal activity, there is clearly a geopolitical dimension to cyber security developments in the region, particularly with respect to China. The passage of a new National Security Law and Anti-Terrorism Law and the publication of a draft Cyber Security Law pushed China to the forefront of developments in cyber security regulation. In China as elsewhere, industry sector regulation has been key to the growing compliance burden. China's banking and insurance regulators have both issued stringent technology risk management guidelines directing institutions to adopt quotas for "secure and controllable" technologies.

Banking regulators in Hong Kong and Singapore, two of the region's financial services hubs, both issued directions to their authorised institutions highlighting the increasing urgency of the need to address cyber security risks. Institutions in both jurisdictions are already subject to detailed technology risk management and data security requirements. The regulatory notices were essentially calling for institutions to go above and beyond these existing requirements and proactively develop solutions to the shifting nature and source of cyber threats.

South Korea has long been home to challenging technical cyber security regulation and data localisation requirements, but now we see these impulses elsewhere. Indonesia, for example, has already moved to enact a data localisation law that will have significant impact on businesses operating there from 2017.

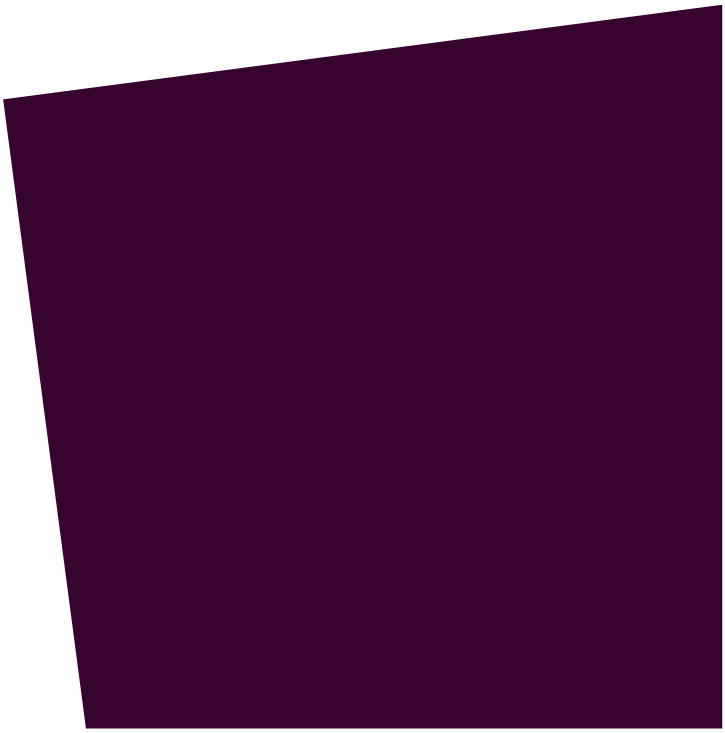
Biometrics, Big Data and the Internet of Things

As data protection regimes mature across the region, we are increasingly seeing lawmakers and regulators crafting regulation and compliance guidance that specifically address data protection aspects of advancing technologies in areas such as biometrics, big data and the internet of things.

In the Asia-Pacific region, as elsewhere, high tech solutions are promising individuals great benefits in terms of quality of life and productivity, but at the same time are raising important data protection and cyber security issues and often running ahead of existing regulations.

Mobile health initiatives, for example, hold promise for improving the efficiency of healthcare delivery in increasingly costly environments of advanced economies and also offer means of extending the scope of healthcare to developing economies that lack the infrastructure to make consistent delivery of basic medical services. These technologies, however, can involve the processing of extremely sensitive personal data.

Biometric data is also playing an increasingly prominent role in combatting cyber security risks, with increasing use of fingerprints, voice authentication and other technologies that seek to improve security controls but at the same time pose a delicate balancing act with respect to data protection interests.



Asia-Pacific region regulators are reacting to these developments. In 2015 we saw Japan introduce a concept of "sensitive personal data" that includes a data subject's medical history. Taiwan broadened its definition of sensitive personal data to include medical records. In both cases the effect is to give health information greater protection under the privacy law.

Hong Kong published detailed guidance on the handling of biometric information, requiring that privacy impact assessments be carried out before such data is used, and that efforts be made to minimise its use in proportion to the objectives.

Japan, Korea and Singapore are all positioning themselves to be regional leaders in Big Data innovations.

Japan's 2015 amendments to its Personal Information Protection Act include specific measures addressing the use of big data and anonymised datasets. South Korea introduced measures addressing many of the same topics in December, 2014.

Singapore's Smart Nation initiative has put a focus on promoting Singapore as a regional hub for developing data analytics and the internet of things, with the Personal Data Protection Commission calling for balance between compliance concerns and space for technological innovation. This balance is reflected in a number of respects under the Singaporean Personal Data Protection Act, which, for example does not apply to publicly available personal data.

We expect to see continuing tensions between the economic development case for advanced data analytics technologies and the data protection risks that these technologies raise, as regulators increasingly turn to issue detailed guidance and take enforcement action.

Asia-Pacific

Data protection regulatory heat map

Our Asia-Pacific Data Protection Regulatory Heat Map is a graphic representation of the relative stringency of the various data protection regulatory regimes across the region.

The map below compares the various regimes in Asia-Pacific by grading jurisdictions against four criteria: 1) data management requirements; 2) data export controls; 3) direct marketing regulation; and 4) the aggressiveness of the enforcement environment. More challenging jurisdictions are represented as red, with less challenging ones appearing as green. We have scored some jurisdictions with striping, reflecting environments with sector-based regulation rather than comprehensive regulation, meaning that the degree of regulation will depend on the specific circumstances of the data being processed.

Asia Pacific

Data export controls

The map below is a graphic representation of the relative degree of regulation of cross-border data transfers across the Asia-Pacific region, with the colour applied to a jurisdiction's borders representing the degree of cross-border restriction in accordance with the legend below. Where a border is marked with a dotted line of alternating colours, the jurisdiction is characterised by sector-specific controls that impose different levels of cross-border regulation.

Individual country spotlights

China

A rapid sequence of legislative reforms in recent years demonstrates a serious resolve by China to move the country towards a more comprehensive data privacy regime, even as abuses of privacy remain stubbornly widespread in its massive and increasingly wired economy.

2015 saw separate but related advances in the area of cyber security regulation. Taken together, we see a greatly sharpened focus for technology use and data management principles for multi-nationals operating in China, particularly in the financial services sector.

In the absence of a dedicated regulator and a unifying legal framework, China's approach to data protection and cyber security matters remains piecemeal. Analysing data privacy issues in China requires a very careful assessment of a number of laws, decisions and guidelines against the specific type of personal data involved and the circumstances of their collection and processing.

The most significant recent development on the data protection side has been the 2014 amendments to the Consumer Rights Protection Law which enshrined data protection principles across the full range of consumer activity. While China has in recent years progressively enacted a fairly significant body of law protecting consumers in the online setting, the 2014 consumer law reforms take China, in practical terms, much closer to a comprehensive approach to regulation.

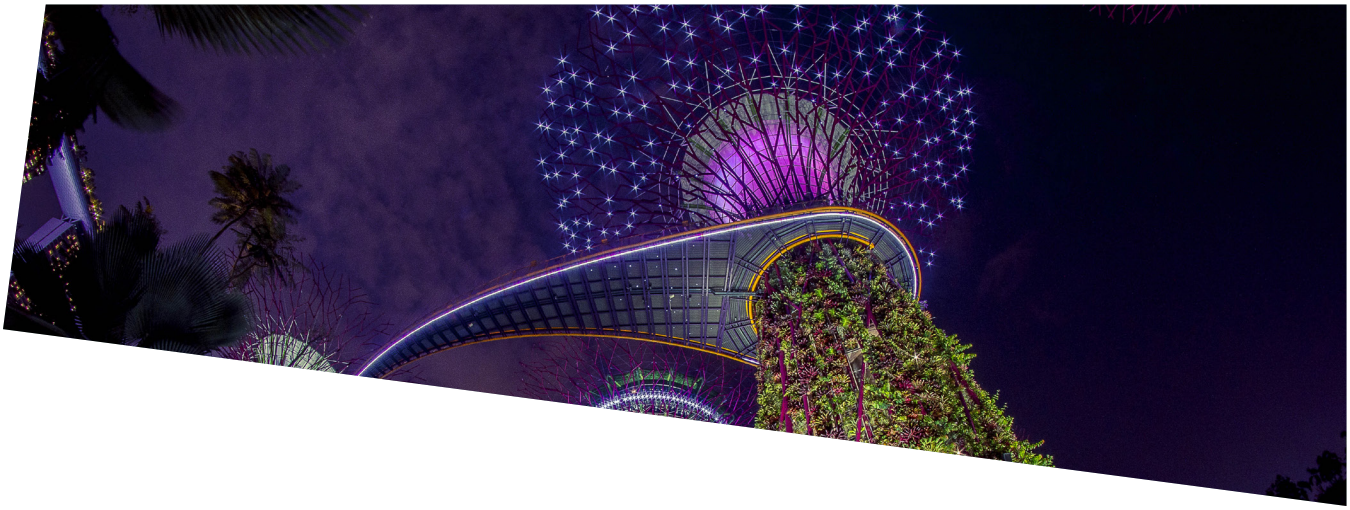
Cyber security regulation dominated international reports of Chinese regulatory developments in 2015. The passage of the National Security Law in July, the publication of a draft Cyber Security Law a few days later and then finally the passage of the Counter-Terrorism Law in December set the stage for an increasingly complex overlay of cyber security regulation. These new laws are directed at a much wider range of issues than data protection, but at the same time introduce elements of data localisation and technology regulation that must be read together with the increasing thicket of data regulation in China in order to properly manage data collection and processing, The banking and insurance sector regulators have at the same time published draft regulations directed at the use of "secure and controllable" technologies that pick up on the same themes found in the new national laws. These reforms may drive multi-nationals to establish separate operating platforms in China making use of local technology. As electronic and mobile commerce and social media continue their explosive growth in China through 2016, we can only expect data protection and cyber security issues to continue to register in China's headlines and policy initiatives. We expect the final form of the banking and insurance regulators' "secure and controllable" regulations to be key to understanding the landscape for China's data protection and cyber security going forward.

Hong Kong

Data privacy regulation has a relatively long history in Hong Kong, with the Personal Data (Privacy) Ordinance (the "PDPO") dating back to 1995. After years of relatively lax enforcement, Hong Kong has stepped to the fore as a policy-making leader on data protection issues in the Asia-Pacific region, with 2015 seeing an increased tendency towards the application of the PDPO's offence provisions.

The Hong Kong Privacy Commissioner for Personal Data's most recent enforcement statistics show a continuing escalation of complaints and enforcement action. Complaints increased 16 per cent year on year to a record high of 1,971. 871,000 Hong Kong individuals were affected by data breaches in 2015, up from 47,000 in 2014. Ninety-eight incidents were reported to the Commissioner last year – a 40 per cent increase year on year – even though Hong Kong's data breach notification regime remains a voluntary one.

Hong Kong saw four convictions under its direct marketing offences. While the fines in these cases were relatively small (HK$5,000 in one case, HK$10,000 in two and HK$30,000 in the fourth), all four prosecutions were widely publicized in the Hong Kong press, underscoring the growing reputational risks for failing to comply with the PDPO.



Hong Kong was caught in the middle of an international data breach incident in November 2015, with the announcement by local toy manufacturer Vtech that customer records of 5 million adults and over 6 million children had been compromised. A well-publicised investigation was also launched into the potential for personal data being taken from contactless credit cards making use of near field communications ("NFC") technologies.

The new Commissioner taking office in August of 2015 has announced an intention to stay at the front of research and policy-making initiatives, with focus on areas such as big data, mobile apps, the internet of things and other electronic data, continuing the regulator's leadership regionally.

Cyber security regulation is also becoming a feature of regulatory considerations in Hong Kong. The banking regulator issued a notice to its regulated institutions in 2015 calling for a stepping up of compliance measures in light of the shifting sources and nature of cyber security threats.

Singapore

Singapore implemented its comprehensive "European-style" Personal Data Protection Act ("PDPA") in two stages in January and July 2014. In the time since, Singapore's new Personal Data Protection Commission has been very active in publishing a significant volume of explanatory guidance for businesses and consumers alike.

Singapore's new law has been enacted with some of the stiffest penalties for data protection offences in the region, with fines of up to S$1 million (USD800,000), but we have yet to see an aggressive approach to enforcement in the island state.

There are economic motives informing the new law, and in this sense Singapore's interpretation of the APEC Privacy Framework may be truer to the accord's stated intentions of promoting e-commerce and cross-border business. Singapore has gone so far as to draw an explicit link between the implementation of data protection regulation and its national ambitions to be a leading high tech hub in the region, including in areas such as data analytics. In January 2016, the government announced an intention to merge the Commission's office with the Infocommunications Media Development Authority, Singapore's telecommunications and broadcasting authority. This move may be seen as a subordination of data protection regulation to Singapore's ambitions to be a Smart City and a haven for technology development.

At the same time, the Singapore government is recognising that cyber security threats pose challenges for these national ambitions. In 2015, the Monetary Authority issued a direction to its authorised institutions to step up their evaluation of and response to cyber security threats. The Ministry of Communications and Industry announced in January 2016 that a new cyber security bill would be put forward as part of a program to manage cyber security risks, drawing a link between the benefits of a smart city and the growing cyber threat.

Japan

Japan's Personal Information Protection Act (the "PIPA") dates back to 2003 and stands as one of Asia's oldest laws in this area. The PIPA is framework legislation that delegates discretion to national administrative agencies and local governments to develop implementing regulations to accomplish the purposes of the law. Following a series of high profile data security breaches and revelations of unlawful sales of personal data in Japan, the Japanese government passed extensive reforms to the PIPA in September 2015. These are the first amendments to the law since its enactment in 2003. The reforms will become fully effective in September 2017.

The main changes include:

- expanding the definition of "personal data" to include biometric information such as fingerprint and face recognition data;
- where personal data has been anonymised, pseudonymised, or otherwise processed so that there is a reduced possibility that the person can be identified, consent of the individual will not be required for the transfer of such data;
- "sensitive" information such as an individual's race, creed, social status and criminal record is now separately protected;
- the establishment of an independent authority to enforce the laws and regulations with stronger enforcement powers; and
- restrictions on the transfer of personal data outside Japan unless contractual provisions are put in place with the overseas recipient to ensure appropriate compliance and prior data subject consent is obtained.

South Korea

South Korea has firmly established itself as one of the toughest jurisdictions for data protection and privacy compliance in the world. Provisions of the over-arching Personal Information Protection Act and the IT Network Act (which regulates the collection and use of personal information by any commercial enterprise that sells or markets its goods or services online) are supplemented by sector-specific laws, creating a very difficult compliance environment. There are extensive registration and disclosure requirements and a need for separate specific data subject consents in areas such as the processing of sensitive personal data, data transfers and data exports. Businesses are obliged to disclose the identities of third party data processors and must report all data security breaches to data subjects and the authorities. Data subject consent is now also required by any business transmitting advertising information by email.

The legislation is also backed up with extensive enforcement measures, including provision for data subject class action suits against offenders. South Korea also has Asia's first revenue-based penalties where fines of up to 3% of revenues can be imposed under the IT Network Act on commercial enterprises selling or marketing goods or services online.

In 2015, South Korea's Ministry of Government Administration and Home Affairs issued an amended version of the Standards of Personal Information Security Measures (the 'Standards'). These Standards seek to close loopholes and inadequacies in the South Korean data protection law and to counter the growing number of data breaches, especially those arising from the use of mobile devices.

The Standards now require that data handlers (data users in Hong Kong parlance) actively supervise manage and monitor outsourcing providers. In addition, 'mobile devices' have been added to the definition of personal information processing systems, and data handlers must ensure that all mobile devices are equipped with appropriate security measures, including the encryption of any personal information stored on them.

Thailand

The Thai government is gearing up for the digital economy and is currently considering nine bills regulating different aspects of that economy. As part of this package of reforms, on 6 January 2015, the Cabinet of Thailand approved a draft data protection bill. Considerable criticism has been raised in public about the draft bill and as a result, the exact date for it to be considered and voted upon by the National Legislative Assembly is not yet known.

One of the main concerns under the draft bill is that personal data may only be collected by the data controller for a lawful purpose directly related to the activities of the person collecting the data. However, critics argue that the draft bill does not draw a distinction between a data controller and a data processor. Without this separation, any third party collecting, using or disclosing personal data on behalf of a data controller could share the same liability and duties of the controller. This approach to regulation would clearly be discouraging for internet service providers, cloud service providers and other participants in the digital economy who process data on others' behalf.

Malaysia

At the time of printing, Malaysia had issued its Personal Data Protection Standards dealing with data security, integrity and retention requirements. Detailed direct marketing guidelines are expected later in 2016 and if these are brought forward in their current form it would introduce controls similar to those in Hong Kong, where specific categories of goods and services and cross-marketing partners need to be identified in the direct marketing consents.

These very specific regulations can be challenging for an increasingly diversified mobile economy, and we understand that the draft has raised considerable debate.

Taiwan

In December 2015, the Office of the President announced a proposal to amend Taiwan's Personal Data Protection Law. It is expected that this proposal will be in force by June 2016. While some of the anticipated changes will enhance data protection in certain aspects, criminal sanctions under the law have been removed and there is broader scope for implied consent to processing "non-sensitive personal data". The definition of "sensitive personal data" has also been broadened to include all medical records and not just information related to treatment, giving health information greater protection under the law.

Indonesia

Indonesia has yet to adopt a comprehensive data protection law but is expected to introduce a draft bill to this effect in the course of 2016. Indonesia's Regulation 82 has introduced a measure of data protection regulation to the country, with particular focus by multi-nationals directed at data localisation measures that will come into effect in 2017. Regulation 82 has threatened significant disruption of regional operating platforms that have tended to host Indonesian data processing operations in jurisdictions such as Singapore, where a more advanced data centre and telecommunications sector can be found.

With a population of over a quarter billion and one of the highest economic growth rates globally, Indonesia is an increasingly important target for multi-national businesses. Accessing this potential is being challenged by an increasingly restrictive regulatory environment for data and technology.

Data Protection and Cybersecurity regulation in Asia:

A guide to making your business compliant

The tightening of Asia's data protection regulatory environment and the emergence of cyber security regulation comes at the same time as personal data has developed into an increasingly valuable business asset. It also comes as regional businesses seek to turn more to outsource data processing and transfer data across borders with a view to improving operational efficiency and leverage economies of scale.

An effective data protection and cyber security compliance program begins with a comprehensive look at the personal data being used within the business and then proceeds to map applicable regulatory requirements to this processing.

At a high level, the steps towards developing an effective compliance plan are as follows:

- What personal data does the business hold and use, how was it obtained and for what purposes is it being processed?
- Is the data being transferred to any other group companies or to unrelated third parties for any purpose? If so, into which jurisdictions is the data being sent?
- What future plans does the business have for processing data, in particular having regard to new business lines, new jurisdictions, new technologies, new business models and other potential new avenues to monetising data?
- What data protection and cyber security regulatory regimes apply to the organisation's personal data holdings, bearing in mind both the location in or from which the data was collected and the location or locations where it is being processed?
- Are the business's existing policies and procedures compliant? Where are the gaps and what are the practical options for achieving compliance?

Each of these steps is explored in more detail below.

A Personal Data Audit

The first step towards developing an effective compliance plan is to understand what personal data the business uses.

Customer Data

Customer databases are one of the more obvious holdings of personal data, particularly for consumer facing businesses. The practical issue for identifying the full extent of an organisation's customer data holdings is that databases are not always clearly marked out as such, particularly now in the era of cloud computing and widespread use of mobile devices.

Engaging with sales, marketing, business development and technology teams is often the key to successfully auditing customer data holdings. Care needs to be taken to understand the specific technologies being used by the business and whether data is being collected or extracted online or through mobile handsets, whether directly or through third party service providers.

Data that has been anonymised or aggregated for profiling or analytics purposes may not, strictly speaking, be "personal data", but this data should nevertheless be included as part of the audit. Data protection laws generally look at data from an entity-wide or group-wide perspective, meaning that de-personalised data sets that can be linked to identities will not avoid compliance requirements. With the proliferation of social media and online public data sources, the risk of "re-identifying" individuals from anonymised or aggregated datasets has never been higher. Assessing data protection compliance will involve assessing the procedures for creating and maintaining the de-personalisation of these datasets.

Employee Data

As Asia region businesses grow in scale and geographic reach, we see a trend towards increased consolidation of human resources databases and increased use of external service providers to administer HR processes and procedures. This development has been running up against stricter data privacy laws in general and, in particular, the imposition of data export controls in a number of jurisdictions – hence the need to be more vigilant and ensure that data holdings have been properly identified and audited.

An important aspect of employee data is that it almost invariably includes "sensitive personal data" such as information about health and ethnic background. Sensitive personal data is subject to enhanced privacy protection under a number of the region's laws.

Other Personal Data

Many organisations will also hold personal data about individuals who are not their direct customers, such as shareholders, directors and company officers of corporate customers and suppliers, as well as family members and other individuals who are connected to customers or employees. In the context of social media and cloud services businesses, there are often holdings of user contacts or "refer a friend" data that has not been directly obtained from the business's customers. This personal data will nevertheless be subject to regulation.

It can very be important to identify data holdings of individuals of this type, given that the business may not have any direct contractual relationship with the individuals concerned, and so find it more challenging to obtain data subject consents and otherwise be sure that compliance requirements have been met.

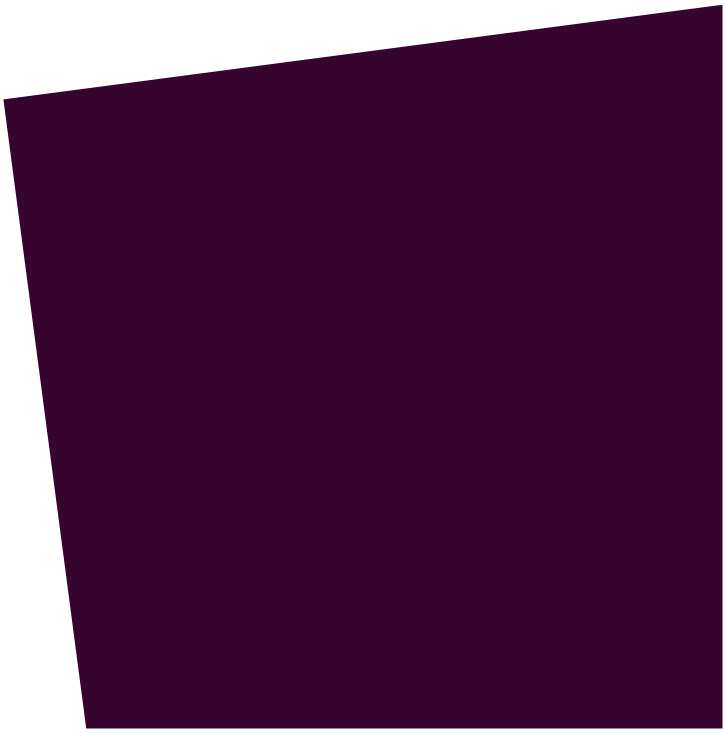
Assessing the Means of Collection and the Purposes for Processing

Once the various personal data holdings within an organisation have been identified, the next task will be to identify how the data was obtained and the purposes for which each group of data is being processed. This will likely again be a matter of engaging with appropriate individuals within functions such as sales and marketing, HR, technology and operations who understand the business processes involved.

As noted above, the pace of technology deployment within an organisation may well run ahead of the legal and compliance teams' immediate understanding of what sort of collection and processing is taking place across the business. Data analytics, for example, is an increasingly valuable business tool across a wide range of industries. It is too often the case that these technologies have been deployed without proper compliance checks.

Another area that can raise difficulties is the use of publicly sourced data. In some jurisdictions, such as Singapore, privacy laws do not in general apply to publicly sourced data. In others such as Hong Kong, regulators have made clear that publicly available data may only be used in compliance with general data privacy principles.

We would recommend a holistic approach to analysing purposes be applied, with references to appropriately stress-tested checklists. New purposes for processing data may develop unexpectedly. For example, it may be a rare occasion that a business has a need to consolidate data on the servers of an e-discovery service provider as part of multi-jurisdictional litigation, but it is much better to be prepared for such an eventuality if it is a practical possibility. Likewise, if personal data may be subject to demands by foreign regulators, care will need to be taken to understand this risk in order to factor in appropriate data subject consents and policies and procedures around data handling if the business is in the position to make the disclosure.



Mapping Data Transfers

A related task in the fact gathering process is to understand where personal data is being transferred to from its points of collection, both in terms of transfers to entities within the wider business group and transfers to unrelated third parties. The geographic transit of personal data will also be important given the proliferation of data export controls across the Asia-Pacific region.

Data transfers can broadly be of two types – (i) transfers to affiliated companies and business partners who collaborate in determining the purposes for data processing or have the discretion to pursue different purposes of processing data (i.e., "controller to controller" transfer scenarios); and (ii) "controller to processor" scenarios in which the transferee simply processes the data in accordance with the transferor's instructions with no discretion to pursue new purposes for processing.

Both types of transfer will be relevant, although the compliance requirements will differ significantly in each case.

Cross-border transfers of personal data raise an additional layer of complexity in many jurisdictions in the Asia-Pacific region which now have data export controls.

Data Maintenance and Retention

Databases constantly evolve through their use, and so an understanding of how a database is updated, corrected and augmented is key to an effective regulatory analysis.

As the Asia-Pacific region's data protection laws are all consent-based, a key consideration is what procedures are in place to ensure that requests from data subjects that processing cease are appropriately addressed.

Similarly, many of the regimes across the region have express data subject access and correction rights. Businesses will be expected to have policies and procedures in place to manage these requests.

As a general rule, the region's laws also oblige businesses to cease processing personal data once the purposes for which it has been collected have been exhausted. There are few prescriptive data retention periods under general purpose data protection laws, but businesses will need to undertake an appropriate analysis to determine how long data should be kept. Likewise, it will be important to evaluate approaches to securely erasing personal data once the purposes for having it have been fulfilled.

An Eye to the Future

While much of the personal data audit process is a forensic one aimed at generating a clear snapshot of the current state of data process across a business organisation, a well-executed review will also consider planned extensions of the purposes for processing of data and changes to business operations, such as plans to consolidate databases and deploy new technologies, such as the introduction of remote access by employees to cloud based services, the "bring your own device" policies and the introduction of behavioural profiling technology to company web sites and apps.

Assessing Regulatory Requirements

Once the organisation's personal data holdings and processing have been understood as a factual matter to a sufficient level of granularity, an analysis against applicable data protection and cyber security regimes can be undertaken.

1. Leveraging what's already there

   The regulatory analysis will not necessarily be a matter of re-inventing the wheel, in particular for European-based multinationals who have invested years of effort in constructing policies and procedures that meet European standards. European standards often (but do not always) meet or exceed national requirements across many jurisdictions in the Asia-Pacific region, and so it is often efficient to leverage global or regional policies from elsewhere in the organisation if they are transportable having regard to the nature of the business and the data processing taking place. As Asia's data protection and cyber security regimes proliferate and develop, however, there are more and more local distinctions that will need to be taken into account.

2. A regional approach to compliance

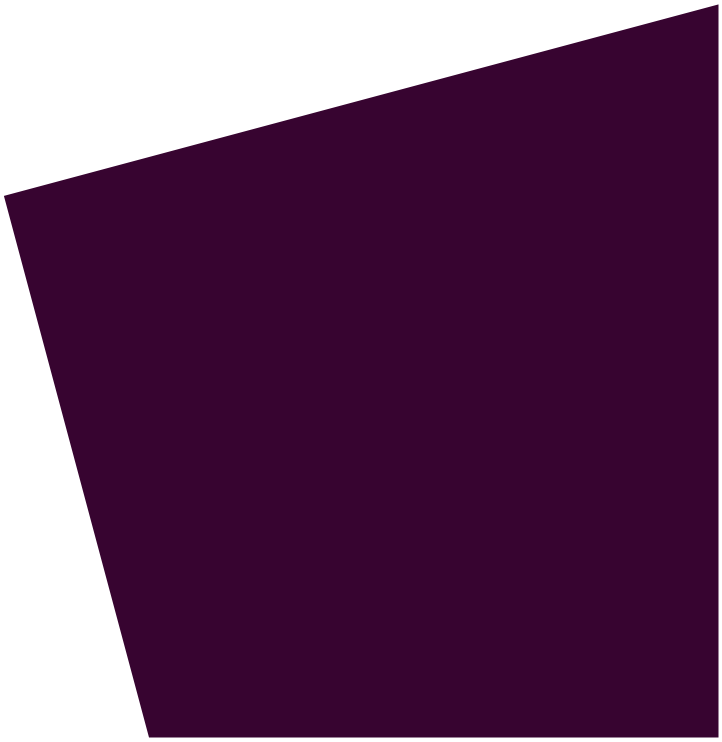
   Irrespective of the starting point a business finds itself in, we generally counsel clients with regional footprints to take a regional view of Asia-Pacific's data protection and cyber security compliance requirements. Although there are important differences at every turn, there is a degree of general conformity, at least, around the principles set out in the APEC Privacy Framework.

   "Levelling up" to APEC standards in jurisdictions without data protection laws often makes good business sense, given the obvious trend towards comprehensive regulation. We expect, for example, new laws to emerge in Indonesia and Vietnam in the coming years, and it is a virtual certainty that the new national laws there will take approaches to regulation that are similar to that taken by their neighbours.

   There is also, of course, good business sense in having a strong brand for data privacy wherever the business may be. In the area of electronic and mobile commerce and payments, borderless data transfers, cloud computing and remote access to databases, a global or regional approach to managing data security and data privacy is becoming increasingly a business necessity.

   While Asia has a number of jurisdictions that are yet to implement legislation tracking the requirements of the APEC Privacy Framework, Asia also has a number of jurisdictions sitting at the other end of the compliance spectrum. South Korea, for example, has marked itself out as being one of the world's most challenging jurisdictions for data privacy compliance. There are other challenges across the region, such as Hong Kong's direct marketing controls and Indonesia's data export requirements. China raises a unique overlay of difficult laws and regulations that pose compliance challenges on a number of fronts. The "new normal" for Asia-Pacific data privacy compliance is setting an ever increasing bar for compliance.

Cyber security regulation is steadily introducing new variables to approaches to data management in the Asia-Pacific region. China's move to require that businesses use "secure and controllable" technology is beginning to drive businesses in regulated sectors in particular to localise technology and data to the mainland. Indonesia's Regulation 82, due for implementation in 2017, is forcing the same considerations there.



Typical Compliance Considerations

The typical range of compliance measures that most businesses will need to turn to will include:

- Personal information collection statements (PICS) prepared either as consents or notifications, as applicable, incorporated into customer terms and conditions, privacy policies for web sites and apps, employment terms and conditions and other interfaces with data subjects.
- Data processing policies and procedures for internal stakeholders to understand and administer, including policies and procedures dealing with:
  - **Data collection and capture**, including policies concerning the use of appropriate PICS and the mechanics of collecting consents and the usage of third party data sources;
  - **Direct marketing**, including alignment of PICS with direct marketing activities, implementation of "opt in"/"opt out" mechanisms, prior consultation with applicable "Do Not Call" registries and compliance with direct marketing formalities, such as consumer response channels and any required "ADV" indicators;
  - **Human resources management**, including policies dealing with job applicant data, retention of and access to employee files, notification and consent to data privacy policies, employee monitoring, management of sensitive employee data and the use of external vendors for functions such as payroll and counselling;
  - **Data analytics**, including policies specifying the types of profiling data that may be used, anonymisation/aggregation principles and policies around "enhancing" datasets through the use of publicly available data or third party datasets;
  - **Data commercialisation**, which looks more broadly for the potential use of the organisation's data to collaborate with other businesses in marketing initiatives and consumer profiling;
  - **Security**, including technical standards applicable to various types of internal and external data processing, data access and permissioning, the use of encryption technologies and policies around the use of data in cloud services and other technologies;
  - **Business continuity and disaster recovery**, including data back-up procedures, the use of redundant storage and contingency planning;
  - **Data subject access**, including procedures for assessing and verifying requests, considering the legal implications of requests and managing costs of responding to requests;
  - **Complaints handling**, including complaints from customers, employees and other affected individuals;
  - **Data quality management**, including procedures for updating and correcting databases and determining if data is to be erased;
  - **Data processing and outsourcing**, including vendor due diligence policies and standard contract clauses and templates for onshore and offshore processing;
  - **Data retention**, including policies for determining how long data of various types are to be retained and how it is to be securely destroyed;
  - **Cyber threat assessments and incident response planning,** including programs to identify and review cyber threats across the organisation, allocation of responsibilities for escalation of and response to incidents;
  - **Data breach management**, including policies for escalating, containing and remediating data breaches and evaluating the need for regulatory or data subject notifications, as well as procedures for assessing any need for change to policies and procedures following the occurrence of a breach; and
  - P**rivacy impact assessment**, which includes a general framework for the organisation to assess privacy impacts due to proposals for organisational, technological or policy change.

Management oversight and review:

Developing effective data protection and cyber security risk management policies and programs will involve engagement with the right stakeholders across the organisation and creating an effective governance regime for approving, overseeing, implementing and reviewing the various policies. The appointment of official roles such as a Data Protection Officer is becoming more common as best practice in the region, even in jurisdictions where the designation is not required by law.

Regulators in the region are becoming increasingly conscious of the degree to which data protection and cyber security policies have been prepared under senior management and board direction. Input from such high levels lends credibility to the compliance effort. Effective implementation of data privacy policies will need to consider appropriate channels for reinforcement of new policies following their publication. Training of individuals within the organisation will be necessary in order to lend context and emphasise the importance of compliance to the business. The policies will need to be seen to have been acted upon in order to be evidence of due compliance, and so enforcement procedures will be critical. Policy breaches will need to be examined after the fact with a view to understanding whether or not any organisational change is needed in response.

In order to be effective, an organisation's data privacy policies will need to be under regular review, reflecting changes in law and regulation, changes in the data being collected and used and changes in technologies and operating procedures. The benefit of experience must also be brought to bear.

Our Asia Pacific practice

At Hogan Lovells we bring an international perspective to advising clients on Asia's data protection and cyber security laws and the ongoing development of policy across the region.

Our Asia Pacific team includes practitioners who practised data privacy law in Europe, and so bring a depth of experience to interpreting Asia-Pacific laws that have a common origin in the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. At the same time, our experts are on the ground in the region and rooted in the local law and language, sensitive to the important emerging local nuances.

Our Asia team is closely integrated with our international team of data protection and cyber security practitioners, and so benefits heavily from a wider team of market-leading lawyers who are at the forefront of policy developments in Europe and the United States, advising clients on the most critical mandates on a world-wide basis.

Where Hogan Lovells does not have offices in the Asia-Pacific region, we have strong working relationships with local counsel experts. These relationships have developed over the course of the effective lifetime of these emerging laws, supporting the delivery of a uniformly consistent and high quality work product and practical solutions for business.

Our Asia data protection and cyber security team is also closely integrated with other relevant specialists, in particular lawyers engaged in commercial arrangements concerning data commercialisation and processing and employment law specialists. Our seamlessness on this front means that we bring a very practical, solutions-based approach to counselling that is well informed by market practice.

Our advice covers all aspects of data protection and cyber security compliance, including:

- Conducting data protection and cyber security compliance audits and developing policies, including integrating Asia policies with existing international policies;
- Helping clients structure and allocate risk in relation to cross-border data transfers, including as part of outsourcing, shared services and cloud arrangements;
- Advising on the acquisition of personal data as an increasingly important part of merger and acquisition and joint venture activity;
- Advising on data protection issues arising from online data capture, whether as part of electronic and mobile commerce, behavioural profiling or otherwise;
- Advising on commercial arrangements, such as marketing, distribution and sponsorship agreements, where securing rights to use personal data is a key business objective;
- Advising on cyber-security regulation and cyber-readiness planning;
- Advising on data breach notification requirements when data is hacked or lost;
- Advising on data subject access requests;
- Defending companies against enforcement actions; and
- Bringing to bear the knowledge and experience of our extensive and market-leading data protection and cyber security management team across the world in finding solutions that work in Asia based on lessons learnt elsewhere.

Key contacts

Hong Kong

Mark Parsons
Partner
T +852 2840 5033
mark.parsons@hoganlovells.com

Eugene Low
Partner
T +852 2840 5907
eugene.low@hoganlovells.com

Beijing

Jun Wei
Partner
T +86 10 6582 9501
jun.wei@hoganlovells.com

Sherry Gong
Counsel
T +86 10 6582 9516
sherry.gong@hoganlovells.com

Japan

Hiroto Imai
Partner
T +81 3 5157 8166
hiroto.imai@hoganlovells.com

Shanghai

Philip Cheng
Partner
T +86 21 6122 3816
philip.cheng@hoganlovells.com

Andrew McGinty
Partner
T +86 21 6122 3866
andrew.mcginty@hoganlovells.com

Singapore

Stephanie Keen
Partner
T +65 6302 2553
stephanie.keen@hoganlovells.com

Vietnam

Jeff Olson
Partner
T +84 8 3825 6370
jeff.olson@hoganlovells.com

Our global Privacy and Cybersecurity practice

Realizing the true value of data

Finding the right balance between the most fruitful use of data and the protection of privacy is one of the greatest challenges of our time. Personal information is an extremely valuable asset and its responsible exploitation is crucial for the world's prosperity.

For that reason, our approach is to look at privacy compliance and information governance as part of our clients' strategic vision for success. Embracing privacy, data protection, and cybersecurity can be crucial in order to gain competitive advantage, because it will promote employee and customer loyalty, encourage consistency and efficiency, and facilitate international expansion. In addition, we believe that privacy is not only compatible with innovation, but can make a valuable contribution to it.

With its depth of knowledge and global presence, Hogan Lovells' Privacy and Cybersecurity team is uniquely placed to help clients realize this potential. We have extensive experience of assisting clients with multi-jurisdictional projects and understand the complexities involved in dealing with laws and regulators across the world. We offer:

- A true specialist practice focused on privacy, cybersecurity, data protection, and information management
- Thought leadership and close involvement in the development and interpretation of the law
- Seamless global coverage through our well established and continuously developing team
- Advice which goes beyond achieving compliance and adds value to the information held by organizations
- A one stop shop for all of your data privacy needs around the globe.

How we can help

We have had a team specializing in Privacy and Cybersecurity for over 25 years. Today Hogan Lovells has one of the largest and most experienced Privacy and Information Management practices in the world, spanning the United States, Europe, and Asia. We assist clients with all of their compliance and risk management challenges, drafting policies and providing advice on legal issues, risk management strategies, and strategic governance. We play an important role in the development of public policy regarding the future regulation of privacy. Additionally, we provide the latest privacy and data protection legal developments and trends to our clients via our blog, Chronicle of Data Protection (http://www.hldataprotection.com).

"A premier data protection practice"

Chambers Global, 2014

"They provide global perspectives and a practical approach, and have a real breadth of experience."

Chambers Global, 2014

Alicante
Amsterdam
Baltimore
Beijing
Brussels
Budapest
Caracas
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jeddah
Johannesburg
London
Los Angeles
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Rio de Janeiro
Riyadh
Rome
San Francisco
São Paulo
Shanghai
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington, D.C.
Zagreb

Our offices
Associated offices

www.hoganlovells.com